Claims

[c1] What is claimed is:

1. A method for updating a ciphering key used in a network system, the network system comprising:

a server for storing registration data;

an access point connected to the server for transmitting data received from the server via wireless transmission and receiving data transmitted via wireless transmission; and

a station for transmitting data to the access point via wireless transmission and receiving data transmitted from the access point via wireless transmission, the station storing a first ciphering key;

the method comprising:

the access point transmitting a first challenge text to the station via wireless transmission;

the station using the first ciphering key stored in the station to encrypt the first challenge text into a first response text;

the station transmitting the encrypted first response text back to the access point via wireless transmission;

the access point comparing the first response text with a first predetermined text;

the station transmitting identification data to the access point when the first response text matches the first predetermined text;

the access point transmitting the identification data of the station to the server; and

the access point transmitting a second ciphering key to the station for replacing the first ciphering key when the identification data matches the registration data.

[c2] 2. The method of claim 1 wherein the second ciphering key is encrypted by the first ciphering key before being transmitted to the station.

[c3] 3. The method of claim 1 wherein the station uses the second ciphering key to encrypt the data transmitted to the access point and to decrypt the data received from the access point after the first ciphering key is replaced by the

second ciphering key.

[c4] 4. The method of claim 1 wherein the station uses the second ciphering key to encrypt the data transmitted to the station after the access point transmits the second ciphering key to the station.

[c5] 5. The method of claim 1 wherein the first predetermined text is generated from encrypting the challenge text by the first ciphering key.

[c6] 6. The method of claim 1 further comprising requesting a response from a user of the station before replacing the first ciphering key by the second ciphering key.

[c7] 7. The method of claim 1 wherein the network comprises a plurality of stations, and each station comprises the first ciphering key.

[c8] 8. The method of claim 1 wherein further comprising:
the access point transmitting a second challenge text to the station via wireless transmission after the second ciphering key is transmitted to the station;
using the second ciphering key stored in the station to encrypt the second challenge text into a second response text;
transmitting the second response text back to the access point via wireless transmission; and
the access point comparing the second response text with a second predetermined text.